Title (en)

SECRET DISTRIBUTION SYSTEM, DISTRIBUTION DEVICE, DISTRIBUTION MANAGEMENT DEVICE, ACQUISITION DEVICE, PROCESSING METHODS FOR SAID DEVICES, SECRET DISTRIBUTION METHOD, PROGRAM, AND RECORDING MEDIUM

Title (de)

GEHEIMES VERTEILUNGSSYSTEM, VERTEILUNGSVORRICHTUNG, VERTEILUNGSVERWALTUNGSVORRICHTUNG, ERFASSUNGSVORRICHTUNG, VERARBEITUNGSVERFAHREN FÜR SOLCHE VORRICHTUNGEN, GEHEIMES VERTEILUNGSVERFAHREN SOWIE PROGRAMM UND AUFZEICHNUNGSMEDIUM DAFÜR

Title (fr)

SYSTÈME DE DISTRIBUTION DE SECRET, DISPOSITIF DE DISTRIBUTION, DISPOSITIF DE GESTION DE DISTRIBUTION, DISPOSITIF D'ACQUISITION, PROCÉDÉS DE TRAITEMENT POUR LESDITS DISPOSITIFS, PROCÉDÉ DE DISTRIBUTION DE SECRET, PROGRAMME ET SUPPORT D'ENREGISTREMENT

Publication

EP 2423904 A4 20130626 (EN)

Application

EP 10767169 A 20100423

Priority

- JP 2010057274 W 20100423
- JP 2009106031 A 20090424

Abstract (en)

[origin: EP2423904A1] A secure secret sharing system is implemented. Shares SH(±, h(±)) are generated by secret sharing of secret information separately for each subset SUB(±); each of share management apparatuses PA(±, h(±)) generates a shared secret value DSH(±, h(±)) by performing a common operation to a corresponding share SH(±, h(±)) and common information containing a common value Ã(±) shared in each subset SUB(±); and an acquisition apparatus generates a reconstructed secret value SUBSK(±) by reconstruction processing for each subset SUB(±), using a plurality of shared secret values DSH(±, h(±)) corresponding to the same subset SUB(±), and generates generation information SK by using the reconstructed secret values SUBSK(±).

IPC 8 full level

H04L 9/08 (2006.01); **G06F 21/60** (2013.01); **G06F 21/62** (2013.01); **G09C 1/00** (2006.01); **H04L 9/30** (2006.01)

CPC (source: EP KR US)

G09C 1/00 (2013.01 - KR); **H04L 9/085** (2013.01 - EP US); **H04L 9/3073** (2013.01 - EP US)

Citation (search report)

- [X] US 6363481 B1 20020326 - HARDJONO THOMAS P [US]
- [X] HACHIRO FUJITA ET AL: "Sharing multilevel secrets among groups using concatenation of reed-solomon codes", THE INSTITUTE OF ELECTRONICS, INFORMATION AND COMMUNICATION ENGINEERS GIJUTSU HOKOKU IEICE TECHNICAL REPORT,, vol. 108, no. 472, 9 March 2009 (2009-03-09), pages 65 - 70, XP008157322
- [AD] SHAMIR ET AL: "HOW TO SHARE A SECRET", IP.COM JOURNAL, IP.COM INC., WEST HENRIETTA, NY, US, 30 March 2007 (2007-03-30), XP013119902, ISSN: 1533-0001
- [AD] P. S. L. M. BARRETO, B. LYNN, M. SCOTT: "Proc. SCN '2002", 2003, SPRINGER-VERLAG., article "Constructing Elliptic Curves with Prescribed Embedding Degrees", pages: 257 - 267, XP002241906
- [AD] A. MIYAJI, M. NAKABAYASHI, S. TAKANO: "New Explicit Conditions of Elliptic Curve Traces for FR Reduction", IEICE TRANS. FUNDAMENTALS, vol. E84-A, no. 5, May 2001 (2001-05-01), pages 1234 - 1243, XP001060011
- [AD] JONATHAN KATZ, AMIT SAHAI, BRENT WATERS: "Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products", JOURNAL OF CRYPTOLOGY, 2008, XP008155971
- See references of WO 2010123114A1

Designated contracting state (EPC)

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK SM TR

DOCDB simple family (publication)

EP 2423904 A1 20120229; **EP 2423904 A4 20130626**; **EP 2423904 B1 20150107**; CN 102396012 A 20120328; CN 102396012 B 20140507; ES 2532332 T3 20150326; JP 2013178589 A 20130909; JP 5337238 B2 20131106; JP 5562475 B2 20140730; JP WO2010123114 A1 20121025; KR 101344353 B1 20131224; KR 20120034156 A 20120410; US 2012030464 A1 20120202; US 8549290 B2 20131001; WO 2010123114 A1 20101028

DOCDB simple family (application)

EP 10767169 A 20100423; CN 201080016595 A 20100423; ES 10767169 T 20100423; JP 2010057274 W 20100423; JP 2011510381 A 20100423; JP 2013133392 A 20130626; KR 20117023961 A 20100423; US 201013264445 A 20100423